Incident Post Mortem: 2 RO Credential Phish

Issue Summary

• An RO's credentials (network login name and password) were phished (stolen on the internet).

Timeline

· Issue reported and dealt with on August 13, 2015



Root Cause



Resolution and recovery

• The user's password was reset immediately and investigation started. No evidence that a breach has occurred was found.

- Increase awareness and 16 (2) (c),21 (1) (a)
- Continue the phishing campaign

Incident Post Mortem: 4 RO Phish #2

Issue Summary

• The ROTC were notified by the AC in ED 48015 that they had fallen victim to a phishing attack. The VM was immediately shut down and it was determined that suspicious activities had occurred. The VM was purged, all system were scanned with our security software, 16 (2) (c) and we re-installed the Guest image from the nightly back-up with the assistance

from our colleagues in ITAS.

Timeline

Issue reported August 17, 2015

Root Cause

16 (2) (c)

٠

Resolution and recovery

 Investigation found that the AC had brought their home laptop, plugged it into the ROTC network, then opened their personal webmail, then clicked on a phishing site. With the machine being wiped clean it was difficult to perform more analysis of what happened, but on the network we are all clear.

Corrective and Preventative Measures

Increase awareness and

Incident Post Mortem: 5 Suspicious Employee

Issue Summary

 An employee who had been dismissed had been acting "suspicious" by insisting on taking his allin-one computer with him when he was moved from cubicle to cubicle. After he was dismissed it was decided to investigate.

Timeline

• August 18, 2015 issue was reported to ITSec team

Root Cause

16 (2) (c)

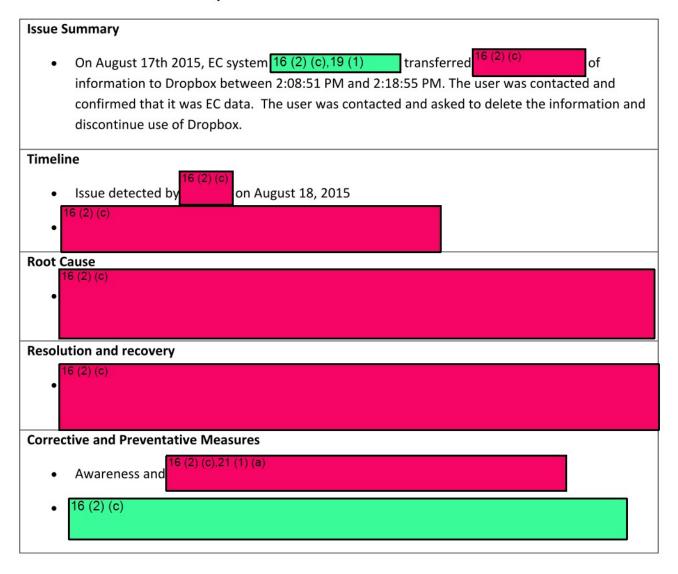
Resolution and recovery

First findings found a VM had been installed, and several pieces of software and media were
downloaded (many illegally) and most likely installed on this VM. No media downloads seemed
to indicate they were illegal other than copyright infringement. Unable to get into VM without
more work. It was decided to end the investigation at that point.

Corrective and Preventative Measures

Increase awareness and

Incident Post Mortem: 6 DropBox issue



Incident Post Mortem: 10 SQL Injection at Bell

Issue Summary Someone posted on Reddit that they successfully performed SQL Injection on an EC production application, which was then tweeted on twitter. They claimed they had reported it to EC (meaning Bell) and that someone had fixed it. Contract App **Timeline**

Issue reported September 9, 2015.

Root Cause Resolution and recovery Investigation found that the SQL injection did happen, although the information gained was not

sensitive. The vulnerable application has been removed and the remaining similar application has had a patch applied 16 (2) (c)

16 (2) (c)

	16 (2) (c),21 (1) (a)
•	
•	
•	
•	
•	
•	

Incident Post Mortem: 13 LiveRail.com

Issue Summary

• 16 (2) (c) alerted the ITSec team that senior individuals in our organization were uploading large amounts of data to an external site without their knowledge. Some of the data was encrypted, and it had gone on at least 7 days and over 600 employees were affected by this situation.

Timeline

• Issue was picked up by on September 11, 2015.

Root Cause

Click-fraud/aggressive online advertising.

Resolution and recovery

• This issue was escalated almost immediately to GC CIRT, who responded by sending someone to collect and analyze data 16 (2) (c)

After much analysis from GC CIRT, 16 and the EC ITSec team it was determined that this was not malware, it was just click fraud (a website creating fake traffic, for profit, at the expense of our bandwidth). During the investigation internet access was shut down to the 10th floor to protect the register and the URL in question was blocked, as well as facebook.

- · LiveRail.com and all other similar style websites are now blocked
- Department-wide ad blocking is being rolled out, via an intake.

Incident Post Mortem: 16 LogMeIn

Issue Summary

Several machines have visited and used logmein.com and other types of services that allow
users to control their machine from home, passing through this external website. This does not
follow our Acceptable Use Policy and also presents a possible security risk.

Timeline

• picked up the activity on September 29, 2015

Root Cause



Resolution and recovery

• LogMeIn.com and some other sites similar to it were blocked.

Corrective and Preventative Measures

Increase IT security awareness, including the AUP and ITSec policies

Incident Post Mortem: 29 IIS Logs Oct 13, Oct 14

Issue Summary		
16 (2) (c) The		
applications in question contained only non-sensitive data, and no data was changed on the server(s).		
Timeline		
October 13, 2015 – SQL injection attack attempts discussed with (2) (c)		
October 14, 2015 – SQL injection attack attempts discussed with 16 (2) (c) 16 (2) (c)		
October 15, 2015 – As there was no way to securely transfer such large files, 16 (2) picked up the files in person		
16 (2) (c) •		
Root Cause		
16 (2) (c)		
Resolution and recovery		
We removed the applications from internet before polling day (October 19, 2015).		
Corrective and Preventative Measures		
16 (2) (c),21 (1) (a)		

Incident Post Mortem: 32 CE15-1016-04 Special Report

Issue Summary

- A report was received from 16 (2) that 3 EC public-facing web applications had had successful SQL injection attempts.
- 2 of the 3 apps had already been reported on previously.
- · All 3 apps contained only non-sensitive data
- No data was changed on the server(s)

Timeline

- Report received October 19th, 2015
- Investigation and reporting completed by October 20, 2015

Root Cause

16 (2) (c) •

Resolution and recovery

We removed the applications from internet before polling day (October 19, 2015).



Incident Post Mortem: 33 CE15-1019-23 ELETC Special Report

Issue Summary

- A java/flash malware was reported to have been downloaded on the EC network, several times.
- · 32 people verified as affected

Timeline

- Issue reported October 19, 2015 (polling day)
- Investigation and notifications complete by October 20, 2015

Root Cause

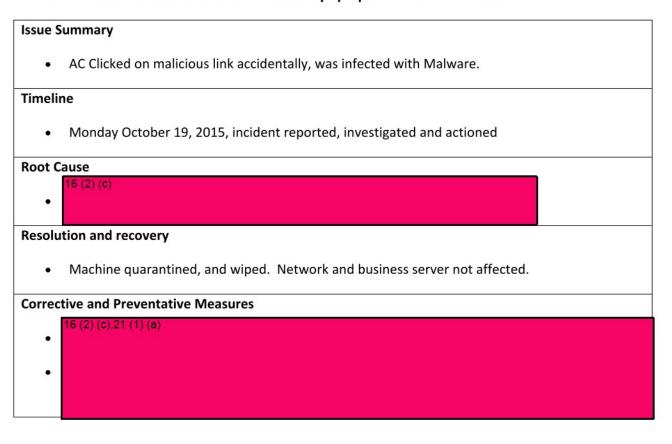
16 (2) (c)

Resolution and recovery

All users who were possibly affected were notified and asked to change all of their web
passwords, work and personal. We also changed several passwords for web applications that
we felt might have been affected, and blocked all sites listed in the report.

Corrective and Preventative Measures

Incident Post Mortem: 34 Malware detected pop up can't close ID: 525633



Incident Post Mortem: 38 Virus-malware at 59037 - AARO3 HV ticket 523179 Lenovo

Issue Summary

• An employee from an AARO office clicked on a phishing link and their machine was believed to be infected with malware.

Timeline

October 18, 2015

Root Cause

· Phishing is common.

Resolution and recovery

• The machine was removed from the network, the user's password was reset. No damage done.

Corrective and Preventative Measures

Sommaire d'incidents enquêtés

Élection Canada 2014 - (16 juin) 2017

2014 (1 incident)

Date	Description	Report Available?
22-Dec-14	Activité suspecte	N

2015 (21 incidents)

Date	Description	Report Available?
01-Jan-15	Activité suspecte	N
13-Aug-15	Hameçonnage	Y (2)
17-Aug-15	Hameçonnage	Y (4)
18-Aug-15	Activité suspecte	Y (5)
18-Aug-15	Activité suspecte	Y (6)
24-Aug-15	Vol d'équipement	Y (36)
30-Aug-15	Vol d'équipement	Y (8)
03-Sep-15	Perte d'équipement	Y (9)
09-Sep-15	Activité suspecte	Y (10)
10-Sep-15	Vol d'équipement	Y (12)
11-Sep-15	Activité suspecte	Y (13)

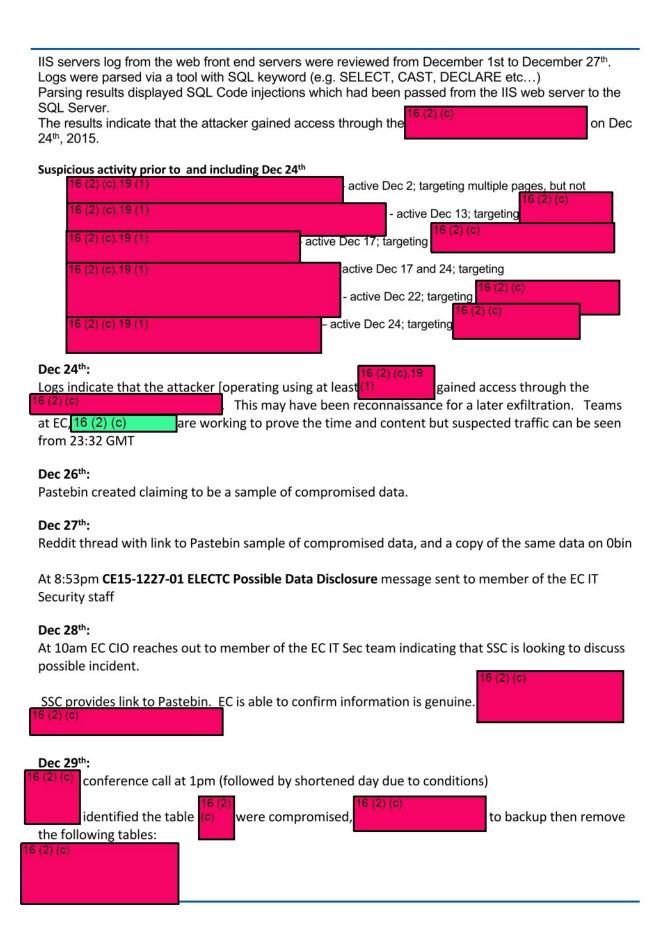
Date	Description	Report Available?
16-Sep-15	Vol d'équipement	Y (15)
29-Sep-15	Activité suspecte	Y (16)
06-Oct-15	Activité suspecte	Y (20)
13-Oct-15	Activité suspecte	Y (29)
15-Oct-15	Activité suspecte	Y (25)
18-Oct-15	Maliciel	Y (38)
19-Oct-15	Activité suspecte	Y (32)
19-Oct-15	Maliciel	Y (33)
19-Oct-15	Maliciel	Y (34)
24-Dec-15	Activité suspecte	Y (A)

2016 (0 incident)

Nul

2017 (0 incident)

Nul



16 (2) (c)	
DAS Le	
	h target dates) 6 (2) (c),19 (1) assessing all 16 (2) (c) HIPS/NIPS logs for SQL injections. (Target Dec 26 and Dec
27 th).	assessing and the control of the con
16 (2) (c)	
1000000	
Dec 30	
Confirm	mation was also received from NHS that the SQL Servers are not accessible via internet. This
provid	es further validation that the vulnerability was a SQL injection.
Implen	nented the following activities to contain the threat (Mtce page posted at 6:00 pm with
	assword and dbases disabled by 7:30 pm) :
	16 (2) (c)
•	
•	Post a maintenance page for the impacted applications.
	16 (2) (c)
	16 (2) (c)
:	
Ĭ.	
ا	This is intended to be in place temporarily until Monday Jan 4 th when the (2) (EC teams can
•	regroup to review the MOP for the proposed changes to the user account/password.
•	Web Server/FW/HIP logs to be sent to 16 (2) (c) at EC. (target dates Dec 26/27 th) Files were
	posted on FTP morning of Dec 31st.
•	Monday Jan 4 th , conference call will be scheduled betwee FEC primes (EC to confirm names) to discuss the plan and impacts to the applications (16 (2) (c)
	names) to discuss the plan and impacts to the applications. 16 (2) (c) 16 (2) (c)

